AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) An asymmetrical key cryptography method involving a processor-implemented keyholder having a number $m \geq 1$ of private keys $Q_1,Q_2,...,Q_m$ and respective public keys $G_1,G_2,...,G_m$, each pair of keys (Q_i, G_i) (where $i = 1,...,m$) satisfying either the relationship $G_i = Q_i^v \bmod n$ or the relationship $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f (where $f > 1$) private prime factors $p_1,\ldots,p_f$, at least two of which are separate, and the exponent v is a public integer equal to a power of 2, wherein the method comprises~~ the steps of~~:

arranging, by a processor, exponent v to have the relationship $v = 2^{b+k}$,

where k is a strictly positive integer and $b = \max(b_1,\ldots,b_f)$, where b_j (where $j = 1,\ldots,f$) is the highest integer such that $(p_j - 1)/2^{bj-1}$ is even; and

arranging, by the processor each public key G_i (where $i = 1,...,m$) to have the form $G_i = g_i^{2^{a_i}}$, mod n ,

where the base numbers g_i are integers strictly greater than 1 and the numbers a_i, are integers such that $1 \leq a_i, \leq b$ and at least one of them is strictly greater than 1.

2. (Previously Presented) A method according to claim 1, wherein at least one of said prime factors $p_1,\ldots, p_f$ is congruent to 1 modulo 4 and the integers a_i (where $i = 1,...,m$) are all equal to said number b .

3. (Previously Presented) A method according to claim 1, wherein said base numbers $g_1,..., g_m$ include at least one number g_s, and said prime factors $p_1,\ldots, p_f$ include at least two numbers p_t and p_u other than 2 such that, given said numbers $b_1,\ldots,b_f$,

if $b_t = b_u$, then $(g_s * p_t) = - (g_s * p_u)$, and

if $b_t < b_u$, then $(g_s * p_u) = -1$,

where $(g_s * p_t)$ and $(g_s * p_u)$ denote the Legendre symbols of g_s relative to p_t and p_u.

4. (Previously Presented) A method according to claim 1, wherein the base numbers $g_1,..., g_m$ are prime numbers.

5. (Currently Amended) A method according to claim 1, involving a processor-implemented controller and said processor-implemented keyholder, here called the process-implemented claimant, wherein the method comprises~~ the following steps~~:

the processor-implemented claimant chooses at random an integer r, calculates the witness $R = r^v \bmod n$ and sends the witness to the processor-implemented controller,

the processor-implemented controller chooses at random m challenges $d_1, d_2, ..., d_m$ and sends the challenges to the processor-implemented claimant,

the processor-implemented claimant calculates the response

$D = r \text{ x } Q_1^{d_1} \text{ x } Q_2^{d_2} \text{ x...x } Q_m^{d_m} \bmod n$,

and sends the response to the processor-implemented controller, and

the processor-implemented controller calculates

$D^v \text{ x } G_1^{\varepsilon_1 d_1} \text{ x } G_2^{\varepsilon_2 d_2} \text{ x...x } G_m^{\varepsilon_m d_m} \bmod n$

where, for $i = 1,...,m$, $\varepsilon_i = +1$ if $G_i \text{ x } Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ if $G_i = Q_i^v \bmod n$, and verifies that the result is equal to the witness R.

6. (Currently Amended) A method according to claim 1, enabling a processor-implemented controller to verify that a message M that it has received was sent to it by said processor-implemented keyholder, here called the processor-implemented claimant, wherein the method comprises~~ the following steps~~:

the processor-implemented claimant chooses at random an integer r and first calculates the witness $R = r^v \bmod n$, then calculates the token $T = h(M ,R)$, where h is a hashing function, and finally sends the token T to the processor-implemented controller,

the processor-implemented controller chooses at random m challenges $d_1,d_2,\ldots,d_m$, and sends the challenges to the processor-implemented claimant,

the processor-implemented claimant calculates the response

$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \ldots \times Q_m^{d_m} \bmod n$ and sends the response to the processor-implemented controller, and

the processor-implemented controller calculates $h\ (M ,D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \ldots \times G_m^{\varepsilon_m d_m} \bmod n)$ where, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ if $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ if $G_i \times Q_i^v \bmod n$, and verifies that the result is equal to the token T .

7. (Previously Presented) A method according to claim 5, wherein the challenges satisfy the condition $0 \leq d_i \leq 2^k - 1$ for $i = 1,\ldots,m$.

8. (Currently Amended) A method according to claim 1, enabling said processor-implemented keyholder, here called the signatory, to sign a message M that it sends to a processor-implemented controller, wherein the method comprises~~ the following steps~~:

the processor-implemented signatory chooses at random m integers r_i , where $i = 1,\ldots,m$, and first calculates the witnesses $R_i = r_i^v \bmod n$, then calculates the token $T = h(M ,R_1,R_2,\ldots,R_m)$, where h is a hashing function producing a word of m bits, and finally sends the token T to the controller,

the processor-implemented signatory identifies the bits $d_1,d_2,\ldots,d_m$ of the token T ,

the processor-implemented signatory calculates the responses $D_i = r_i \times Q_i^{d_i} \bmod n$ and sends the responses to the processor-implemented controller, and

the processor-implemented controller calculates

$$h\ (M, D_1^{v} \times G_1^{\varepsilon_1 d_1} \bmod n,\ D_2^{v} \times G_2^{\varepsilon_2 d_2} \bmod n, \ldots, D_m^{v} \times G_m^{\varepsilon_m d_m} \bmod n)$$

where, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ if $G_i \times Q_i^{v} = 1 \bmod n$ and $\varepsilon_i = -1$ if $G_i \times Q_i^{v} \bmod n$, and verifies that the result is equal to the token T.

9. (Currently Amended) An electronic circuit including a processor and memories, wherein the electronic circuit is programmed to act as said processor-implemented keyholder in executing ~~a~~ the method according to claim 1.

10. (Currently Amended) A dedicated electronic circuit, including microcomponents enabling the electronic circuit to process data in such manner as to act as said processor-implemented keyholder in executing ~~a~~ the method according to claim 1.

11. (Currently Amended) A portable object adapted to be connected to a terminal to exchange data with that terminal, wherein the portable object includes an electronic circuit according to claim 9 or claim 10 and is adapted to store identification data and private keys specific to said processor-implemented keyholder ~~key holder~~.

12. (Currently Amended) A terminal adapted to be connected to a portable object to exchange data with that portable object, wherein the terminal includes a data processing device programmed to act as said processor-implemented controller in executing a method according to any one of claims 5-8.

13. (Currently Amended) A cryptography system comprising:

a portable object adapted to be connected to a terminal to exchange data with that terminal, wherein the portable object includes an electronic circuit,

wherein the electronic circuit is programmed to act as said processor-implemented keyholder in executing an asymmetrical key cryptography method involving ~~a~~ the processor-implemented keyholder having a number m $\geq$ 1 of private keys $Q_1,Q_2,...,Q_m$ and respective public keys $G_1,G_2,...,G_m$, each pair of keys (Q_i, G_i) (where $i = 1,...,m$) satisfying either the relationship $G_i = Q_i^v \bmod n$ or the relationship $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f (where $f > 1$) private prime factors $p_1,\ldots, p_f$, at least two of which are separate, and the exponent v is a public integer equal to a power of 2, wherein the method comprises ~~the steps of~~:

arranging, by the processor, exponent v to have the relationship $v = 2^{b+k}$,

where k is a strictly positive integer and $b = \max(b_1,...,b_f)$, where b_j (where $j = 1,..., f$) is the highest integer such that $(p_j - 1) / 2^{bj-1}$ is even; and

arranging, by the processor, each public key G_i (where $i = 1,...,m$) to have the form $G_i = g_i^{2^{a_i}} \bmod n$,

where the base numbers g_i are integers strictly greater than 1 and the numbers a_i are integers such that $1 \leq a_i \leq$ b and at least one of them is strictly greater than 1,

and wherein the portable object is adapted to store identification data and private keys specific to said processor-implemented keyholder ~~key holder~~; and

a terminal adapted to be connected to the portable object to exchange data with that portable object, wherein the terminal includes a data processing device programmed to act as said processor-implemented controller in executing a method according to ~~any one of claims 5-8~~ claim 6.

14. (Currently Amended) Non-removable data storage means containing electronic data processing program code instructions for, as said processor-implemented keyholder, executing the ~~steps of a~~ method according to claim 1.

15. (Currently Amended) Partially or totally removable storage means containing electronic data processing program code instructions for, as said processor-implemented keyholder, executing the ~~steps of a~~ method according to claim 1.

16. (Previously Presented) A data processing device comprising storage means according to claim 14 or claim 15.

17. (Currently Amended) Non-removable, partially removable, or totally removable data storage means containing electronic data processing program code instructions for, as said processor-implemented controller, executing the ~~steps of a~~ method according to any one of claims 5-8.

18. (Canceled)

19. (Previously Presented) A data processing device, wherein it comprises storage means according to claim 17.

20. (Currently Amended) A cryptography system comprising:

a data processing device including storage means containing electronic data processing program code instructions for, as said processor-implemented keyholder, executing ~~the steps of~~ an asymmetrical key cryptography method involving ~~a~~ the processor-implemented keyholder having a number $m \geq 1$ of private keys $Q_1,Q_2,...,Q_m$ and respective public keys $G_1,G_2,...,G_m$, each pair of keys (Q_i, G_i) (where $i = 1,...,m$) satisfying either the relationship $G_i = Q_i^v \bmod n$ or the relationship $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f (where $f > 1$) private prime factors $p_1,\ldots, p_f$, at least two of which are separate, and the exponent v is a public integer equal to a power of 2, wherein the method comprises ~~the steps of~~:

arranging, by the processor, exponent v to have the relationship $v = 2^{b+k}$,

where k is a strictly positive integer and $b = \max(b_1,\ldots,b_f)$, where b_j (where $j = 1,\ldots,f$) is the highest integer such that $(p_j - 1) / 2^{b_j - 1}$ is even; and

arranging, by the processor, each public key G_i (where $i = 1,\ldots,m$) to have the form $G_i = g_i^{2^{a_i}}$ mod n,

where the base numbers g_i are integers strictly greater than 1 and the numbers a_i are integers such that $1 \leq a_i \leq b$ and at least one of them is strictly greater than 1; and

a data processing device including data storage means containing electronic data processing program code instructions for, as said processor-implemented controller, executing the ~~steps of a~~ method according to any one of claims 5-8.

21. (Canceled).

22. (Previously Presented) A method according to claim 4, wherein the base numbers $g_1,\ldots, g_m$ are chosen from the first 54 prime numbers.